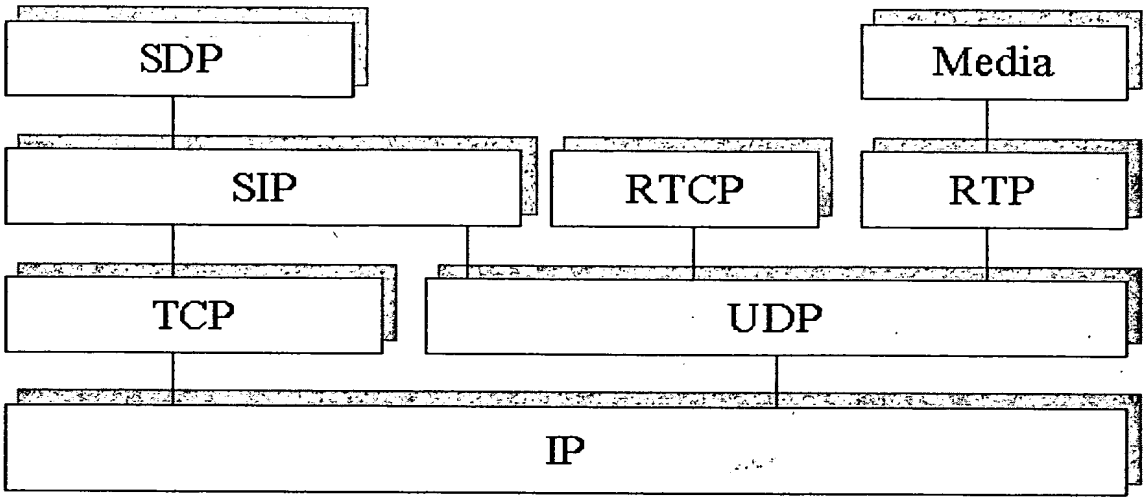


FIG. 1

General header fields	Entity header fields	Response header fields	Request header fields
Accept	Content-Encoding	Allow	Authorization
Accept-Encoding	Content-Length	Proxy-Authenticate	Contact
Accept-Language	Content-Type	Retry-After	Hide
Call-ID		Server	Max-Forwards
Contact		Unsupported	Organization
Cseq		Warning	Priority
Date		WWW-Authenticate	Proxy-Authorization
Encryption			Proxy-Require
Expires			Route
From			Require
Record-Route			Response-Key
Timestamp			Subject
To			User-Agent
Via			

FIG. 2

Session description		k*	Encryption key
Type	Description	a*	Zero or more session attribute lines
v	Protocol version	**Time Description**	
o	Owner/creator and session identifier	t	Time the session is activated
s	Session name	r*	Zero or more repeat times
i*	Session information	**Media description**	
u*	URI of description	m	Media name and transport address
e*	Email address	i*	Media title
p*	Phone number	c*	Connection information – optional if included at session level
c*	Connection information – not required if included in all media	b*	Bandwidth information
b*	Bandwidth information	k*	Encryption key
z*	Time zone adjustments	a*	Zero or more media attributes

FIG. 3

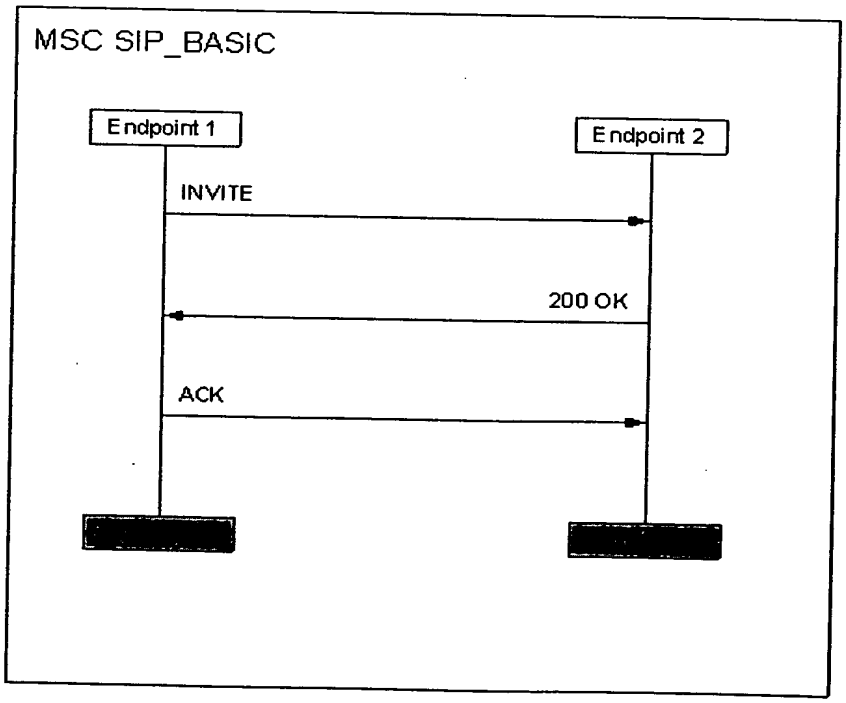


FIG. 4

09/528,428 - 120900

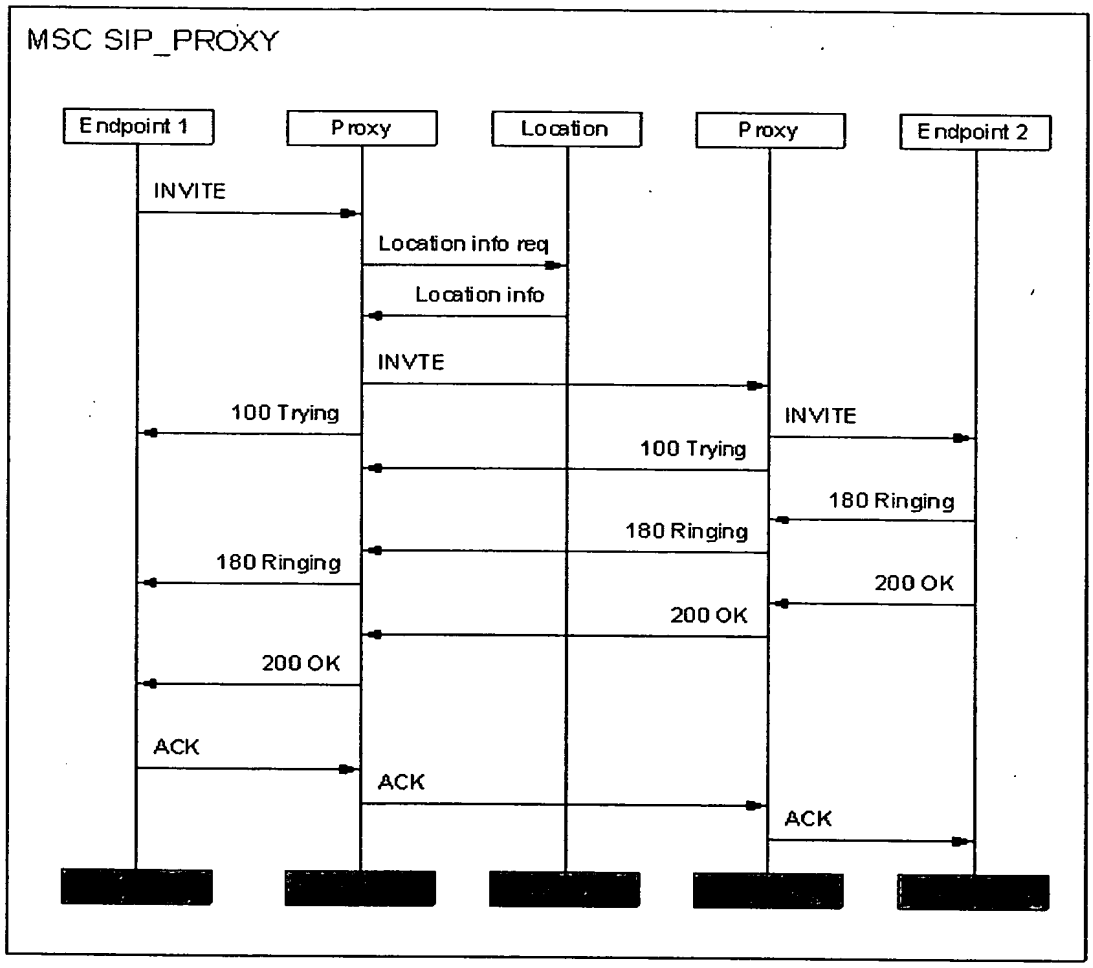


FIG. 5

09/954,268

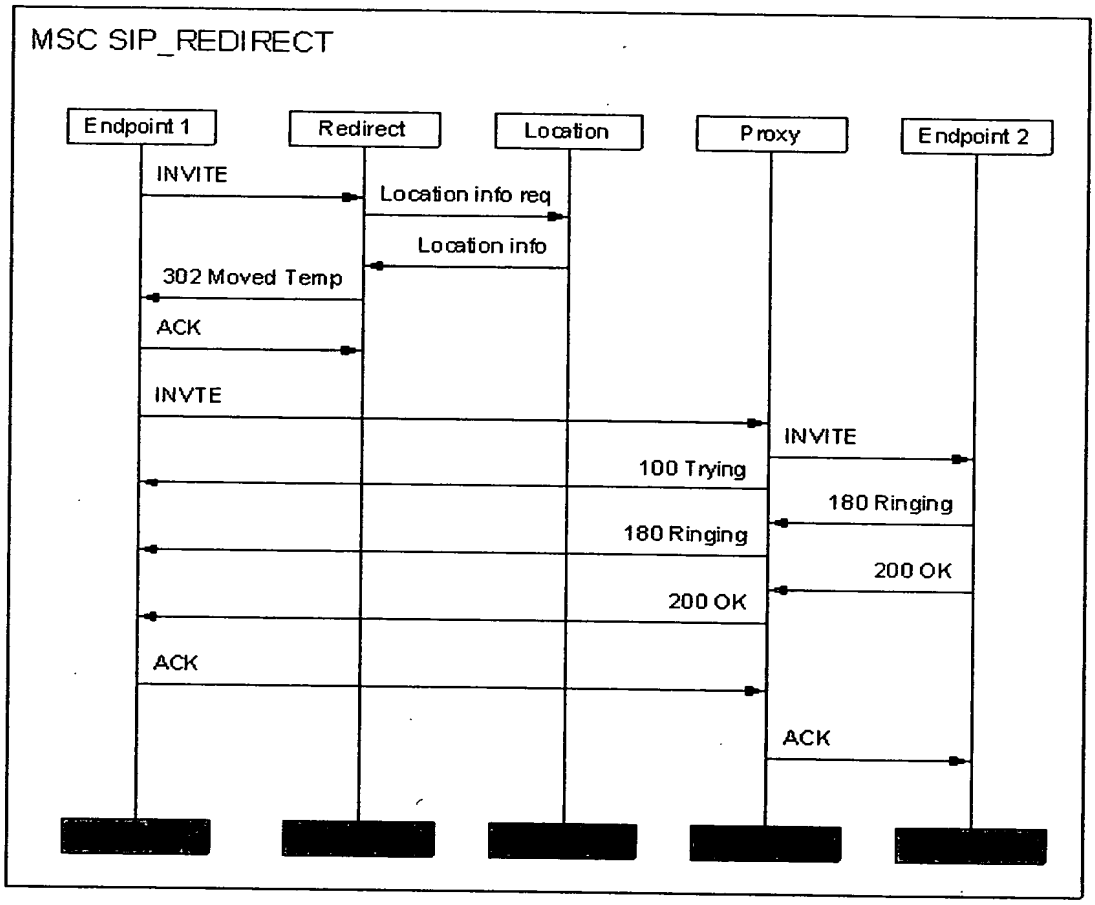


FIG. 6

Access Control	Restricting access to resources to privileged entities.
Authentication	Corroboration of the identity of an entity or the source of information (data origin authentication)
Authorization	Conveyance, to another entity, of official sanction to do or be something
Anonymity	Concealing the identity of an entity involved in some process
Availability	Accessibility of systems and information by authorized users
Certification	Endorsement of information by a trusted entity
Confidentiality or Privacy	Keeping information secret from all but those who are authorized to see it
Confirmation	Acknowledgement that services have been provided
Data integrity	Ensuring information has not been altered by unauthorized or unknown means
Non-repudiation	Preventing the denial of previous commitments or actions
Ownership	A means to provide an entity with the legal right to use or transfer a resource to others
Receipt	Acknowledgement that information has been received
Revocation	Retraction of certification or authorization
Signature	A means to bind information to an entity
Timestamping	Recording the time of creation or existence of information
Validation	A means to provide timeliness of authorization to use or manipulate information or resources
Witnessing	Verifying the creation or existence of information by an entity other than the creator

FIG. 7

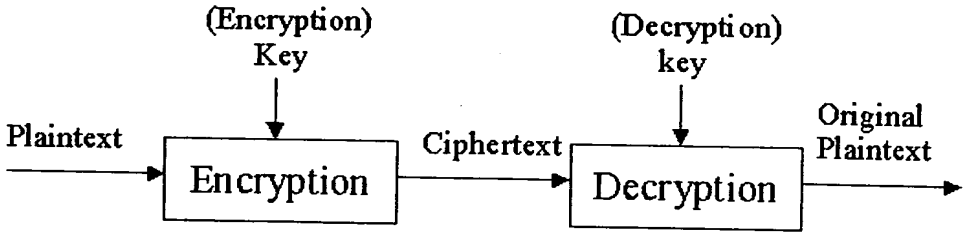

(Encryption)
Key
(Decryption)
key
Plaintext
Encryption
Ciphertext
Decryption
Original
Plaintext

FIG. 8

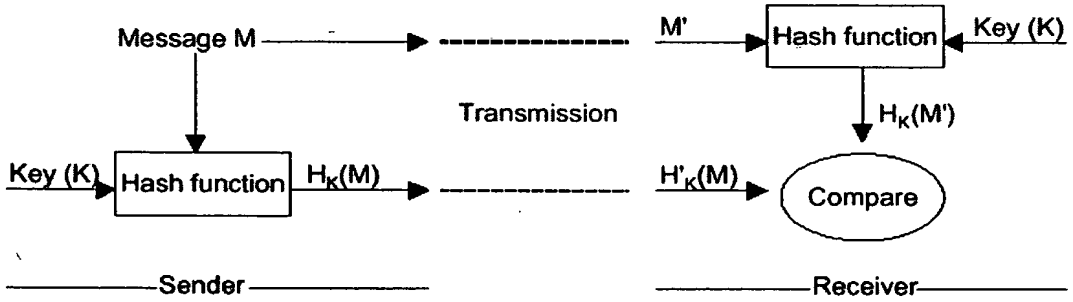

Message M
M'
Hash function
Key (K)
Transmission
$H_K(M')$
Key (K)
Hash function
$H_K(M)$
$H'_K(M)$
Compare
Sender
Receiver

FIG. 9

```
INVITE sip:watson@boston.bell-telephone.com SIP/2.0$
Via: SIP/2.0/UDP 169.130.12.5$
To: T. A. Watson <sip:watson@bell-telephone.com>$
From: A. Bell <sip:a.g.bell@bell-telephone.com>$
Encryption: PGP version=5.0$
Content-Length: 224$
Call-ID: 187602141351@worcester.bell-telephone.com$
Content-Type: message/sip$
CSeq: 488$
$
*********************************************************
* Subject: Mr. Watson, come here.$                      *
* Content-Type: application/sdp$                        *
* $                                                     *
* v=0$                                                  *
* o=bell 53655765 2353687637 IN IP4 128.3.4.5$          *
* s=Mr. Watson, come here.$                             *
* t=0 0$                                                *
* c=IN IP4 135.180.144.94$                              *
* m=audio 3456 RTP/AVP 0 3 4 5$                         *
*********************************************************
```

```
INVITE sip:watson@boston.bell-telephone.com SIP/2.0$
Via: SIP/2.0/UDP 169.130.12.5$
To: T. A. Watson <sip:watson@bell-telephone.com>$
From: A. Bell <a.g.bell@bell-telephone.com>$
Encryption: PGP version=5.0$
Content-Type: application/sdp$
Content-Length: 107$
Call-ID: 187602141351@worcester.bell-telephone.com$
CSeq: 488$
$
************************************************
* $                                            *
* v=0$                                         *
* o=bell 53655765 2353687637 IN IP4 128.3.4.5$ *
* c=IN IP4 135.180.144.94$                     *
* m=audio 3456 RTP/AVP 0 3 4 5$                *
************************************************
```

FIG. 10

09594548 - 120900

The "where" column describes the request and response types with which the header field can be used. "R" refers to header fields that can be used in requests (that is, request and general header fields). "r" designates a response or general-header field as applicable to all responses.

The "enc." column describes whether this message header field MAY be encrypted end-to-end. A "n" designates fields that MUST NOT be encrypted, while "c" designates fields that SHOULD be encrypted if encryption is used.

The "e-e" column has a value of "e" for end-to-end and a value of "h" for hop-by-hop header fields.

Other header fields may be encrypted or may travel in the clear as desired by the sender. The Subject, Allow and Content-Type header fields will typically be encrypted. The Accept, Accept-Language, Date, Expires, Priority, Require, Call-ID, Cseq, and Timestamp header fields will remain in the clear.

	where	enc.	e-e
Accept	R/r		e
Accept	415		e
Accept-Encoding	R/r		e
Accept-Encoding	415		e
Accept-Language	R	e	
Accept-Language	415		e
Alert-Info	R	e	e
Allow	200		e
Allow	405		e
Authorization	R/r		e
Call-ID	gc	n	e
Contact	R	e	o
Contact	1xx		e
Contact	2xx		e
Contact	3xx		e
Contact	485		e
Content-Disposition		e	e

FIG. 11(a)

Content-Encoding		e	e
Content-Length		n	e
Content-Type		e	e
CSeq	gc	n	e
Date	g		e
Encryption	g	n	e
Expires	g	e	
From	gc	n	e
Hide	R	n	h
Max-Forwards	R	n	e
MIME-Version	g	n	e
Organization	g	e	h
Priority	R	c	e
Proxy-Authenticate	401, 407	n	h
Proxy-Authorization	R	n	h
Proxy-Require	R	n	h
Record-Route	R		h
Record-Route	2XX,401,484		h
Require	g		e
Response-Key	R	c	e
Retry-After	R	c	e
Retry-After	404,480,486	c	e
	503	c	e
	600,603	c	e
Route	R		h
Server	r	c	e
Subject	R	c	e
Support	g	c	e
Timestamp	g		e
To	gc(1)	n	e
Unsupported	420	e	o
Unsupported	R		e
User-Agent	g	c	e
Via	gc(2)	n	e
Warning	r		e
WWW-Authenticate	R/401	c	e

FIG. 11(b)

```
INVITE sip:watson@boston.bell-telephone.com SIP/2.0
Via: SIP/2.0/UDP 169.130.12.5
Authorization: PGP version=5.0, signature=...
From: A. Bell <sip:a.g.bell@bell-telephone.com>
To: T. A. Watson <sip:watson@bell-telephone.com>
Call-ID: 187602141351@worcester.bell-telephone.com
Subject: Mr. Watson, come here.
Content-Type: application/sdp
Content-Length: ...

v=0
o=bell 53655765 2353687637 IN IP4 128.3.4.5
s=Mr. Watson, come here.
t=0 0
c=IN IP4 135.180.144.94
m=audio 3456 RTP/AVP 0 3 4 5
```

FIG. 12

```
INVITESIP/2.0From: A. Bell <sip:a.g.bell@bell-telephone.com>
To: T. A. Watson <sip:watson@bell-telephone.com>
Call-ID: 187602141351@worcester.bell-telephone.com
Subject: Mr. Watson, come here.
Content-Type: application/sdp
Content-Length: ...

v=0
o=bell 53655765 2353687637 IN IP4 128.3.4.5
s=Mr. Watson, come here.
t=0 0
c=IN IP4 135.180.144.94
m=audio 3456 RTP/AVP 0 3 4 5
```

FIG. 13

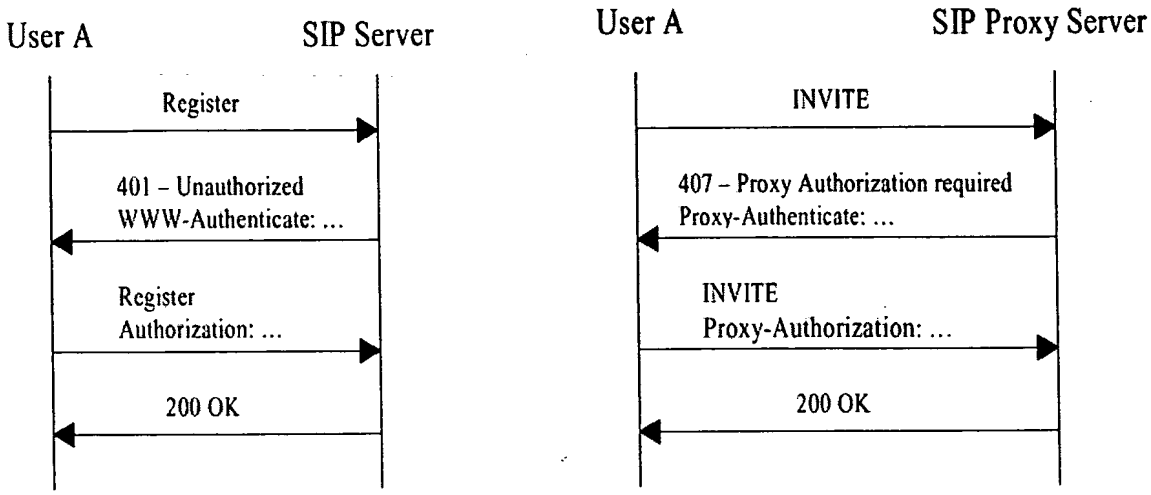

User A
SIP Server
Register
401 – Unauthorized
WWW-Authenticate: ...
Register
Authorization: ...
200 OK
User A
SIP Proxy Server
INVITE
407 – Proxy Authorization required
Proxy-Authenticate: ...
INVITE
Proxy-Authorization: ...
200 OK

FIG. 14

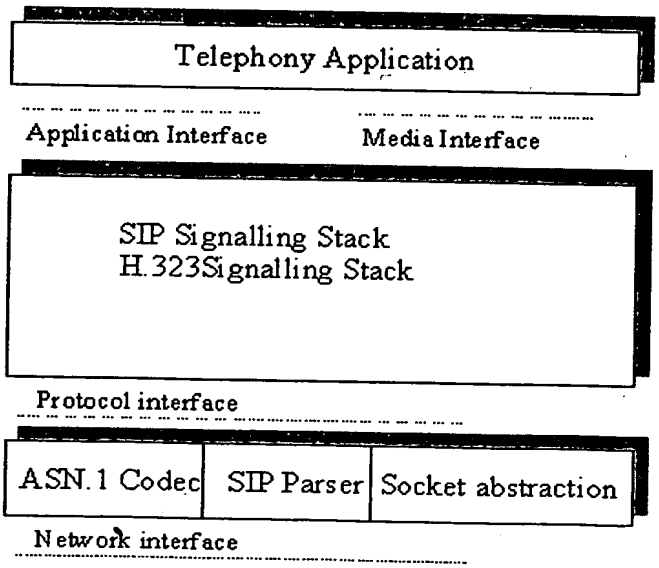

Telephony Application
Application Interface
Media Interface
SIP Signalling Stack
H.323Signalling Stack
Protocol interface
ASN.1 Codec
SIP Parser
Socket abstraction
Network interface

FIG. 15

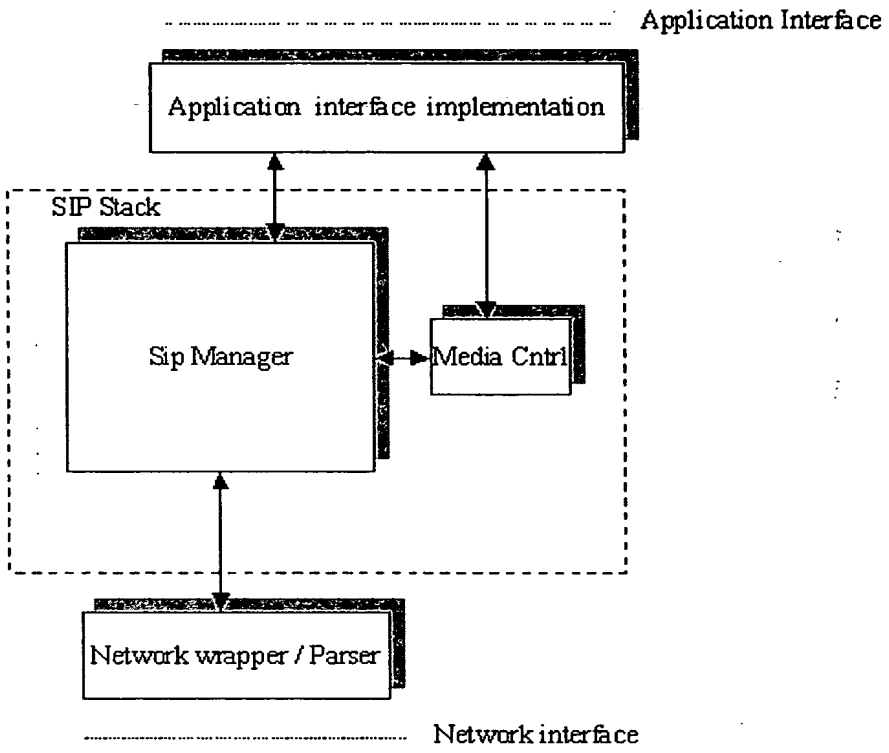

Application Interface
Application interface implementation
SIP Stack
Sip Manager
Media Cntrl
Network wrapper / Parser
Network interface

FIG. 16

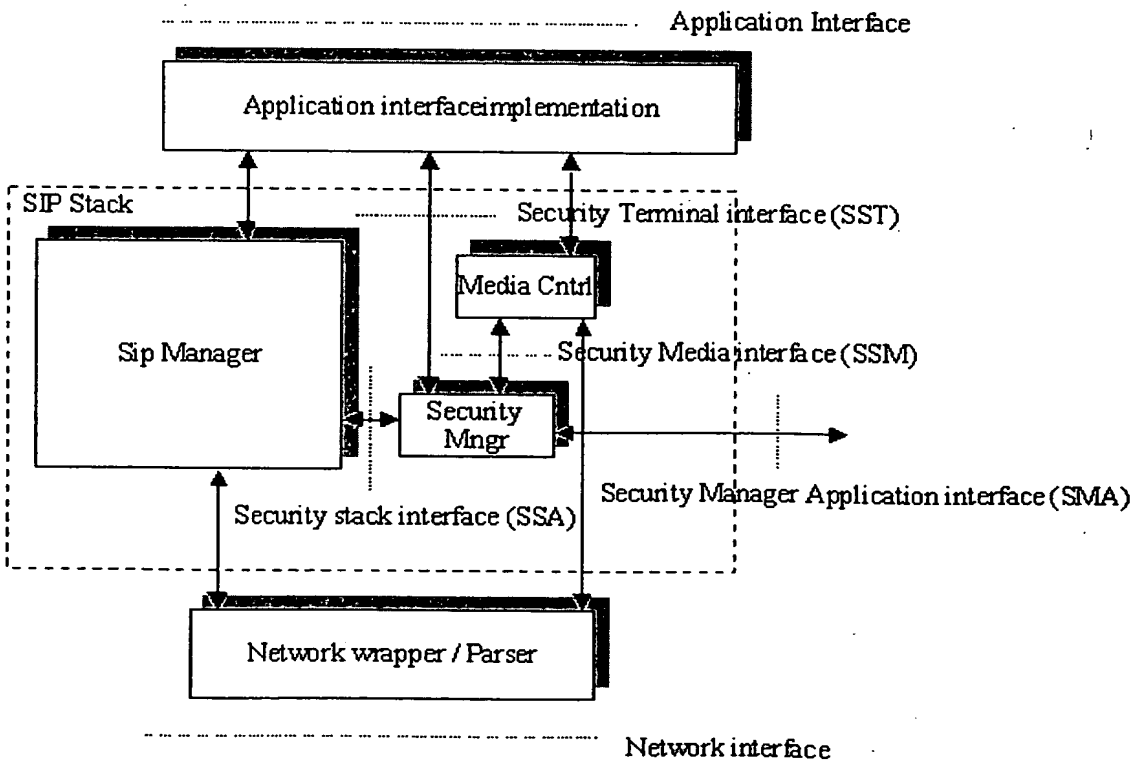

Application Interface
Application interfaceimplementation
SIP Stack
Security Terminal interface (SST)
Media Cntrl
Sip Manager
Security Media interface (SSM)
Security Mngr
Security Manager Application interface (SMA)
Security stack interface (SSA)
Network wrapper / Parser
Network interface

FIG. 17

006227 "24T25760

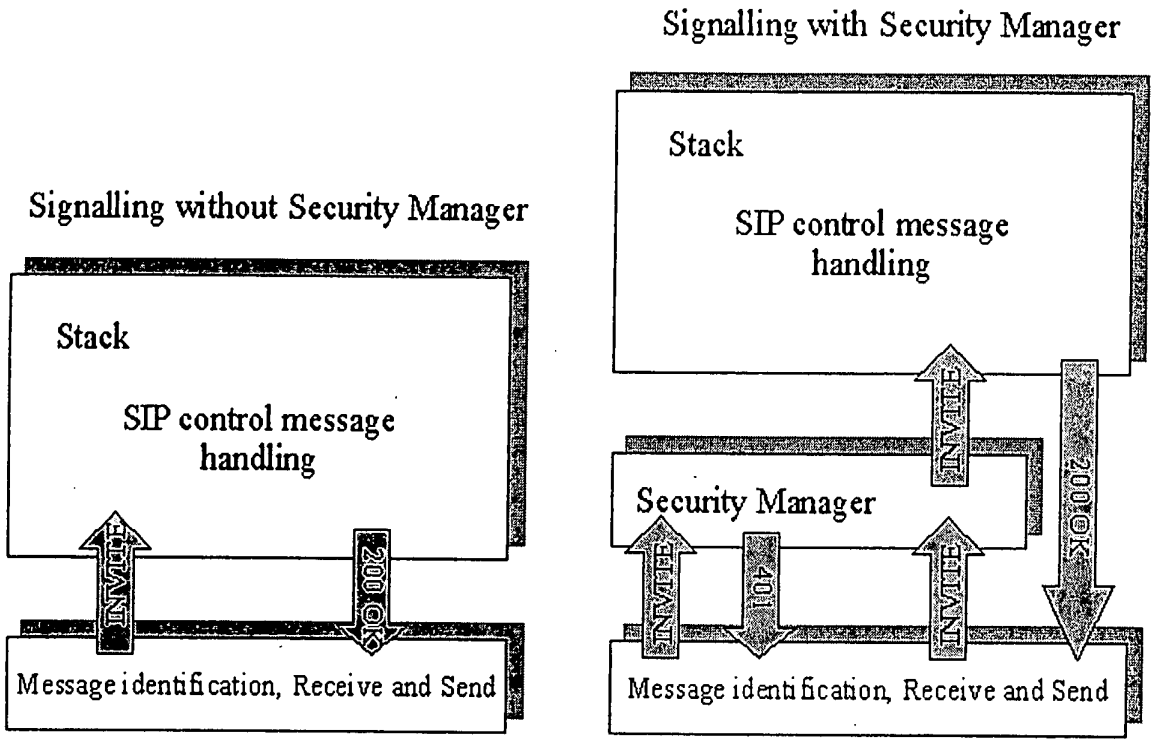


FIG. 18

00622T" 2hT25260

Sending terminal

State before	Signal from stack	Task	State after	Signal to stack	Purpose
Idle	got_unauthorized	TASK_SecurityManager_authorization_reqd	Idle	send_auth_invite	Make authorized message

Receiving terminal

State before	Signal from stack	Task	State after	Signal to stack	Purpose
Idle	sip_invite	TASK_SecurityManager_invite	wait_auth_invite	send_www_auth	Check the incoming invite in Idle state and move to
		TASK_SecurityManager_send_www_auth			wait_auth_invite state, send send_www_auth to the stack
wait_authorized_invite	sip_invite	TASK_SecurityManager_invite	Idle	got_invite	Check the incoming invite in wait_auth_invite state and move
					to idle state (call was authorized) send got_invite to the stack
wait_authorized_invite	sip_invite	TASK_SecurityManager_invite	Idle	error	Check the incoming invite in wait_auth_invite state and move to
		TASK_SecurityManager_error			idle state (call was not authorized) send error
wait_authorized_invite	got_error	TASK_SecurityManager_error	Idle		Handle the error

FIG 19

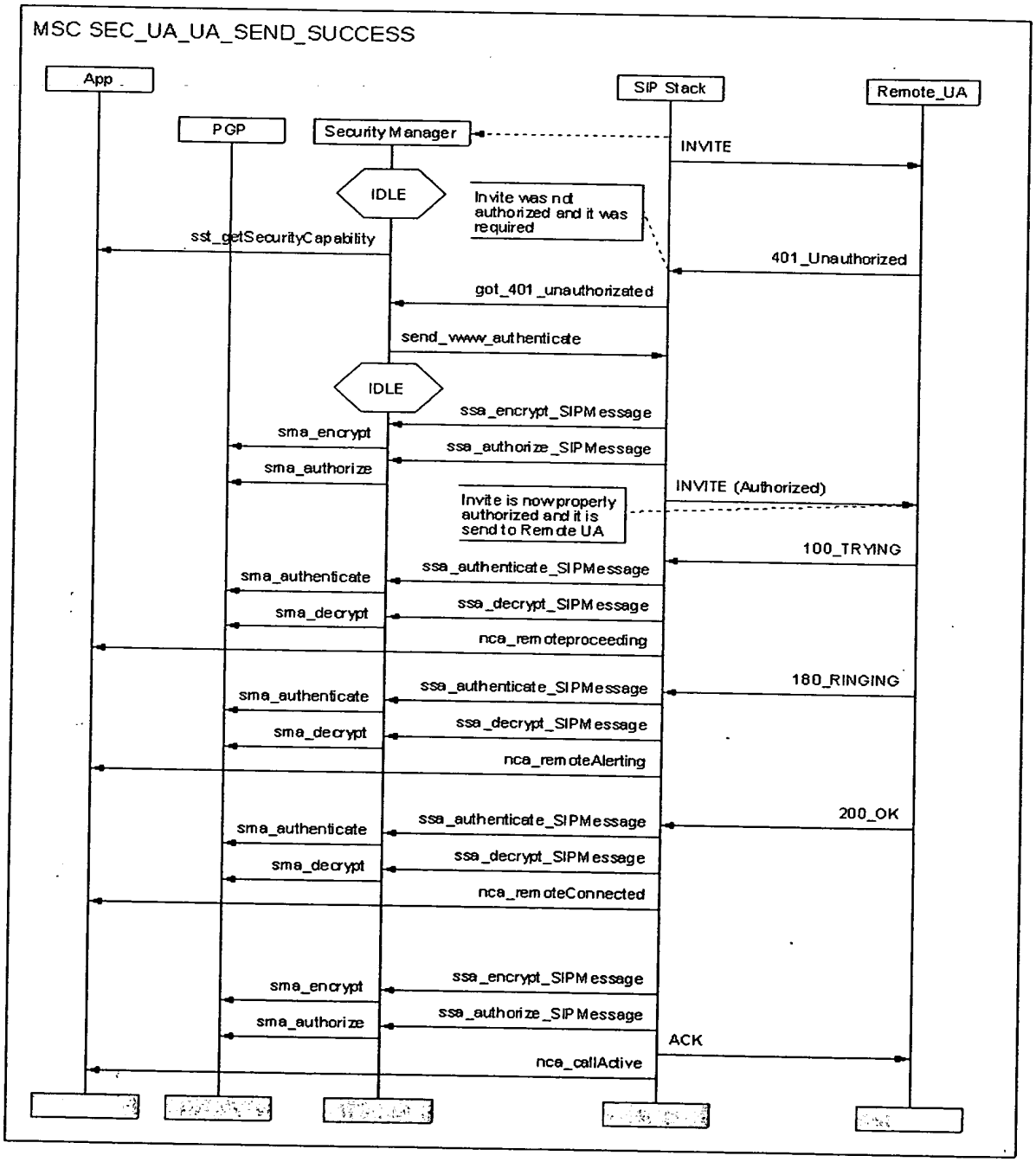

MSC SEC_UA_UA_SEND_SUCCESS
App
PGP
Security Manager
SIP Stack
Remote_UA
INVITE
IDLE
Invite was not authorized and it was required
sst_getSecurityCapability
401_Unauthorized
got_401_unauthorizated
send_www_authenticate
IDLE
ssa_encrypt_SIPMessage
sma_encrypt
ssa_authorize_SIPMessage
sma_authorize
INVITE (Authorized)
Invite is now properly authorized and it is send to Remote UA
100_TRYING
sma_authenticate
ssa_authenticate_SIPMessage
sma_decrypt
ssa_decrypt_SIPMessage
nca_remoteproceeding
180_RINGING
sma_authenticate
ssa_authenticate_SIPMessage
sma_decrypt
ssa_decrypt_SIPMessage
nca_remoteAlerting
200_OK
sma_authenticate
ssa_authenticate_SIPMessage
sma_decrypt
ssa_decrypt_SIPMessage
nca_remoteConnected
sma_encrypt
ssa_encrypt_SIPMessage
sma_authorize
ssa_authorize_SIPMessage
ACK
nca_callActive

FIG. 20

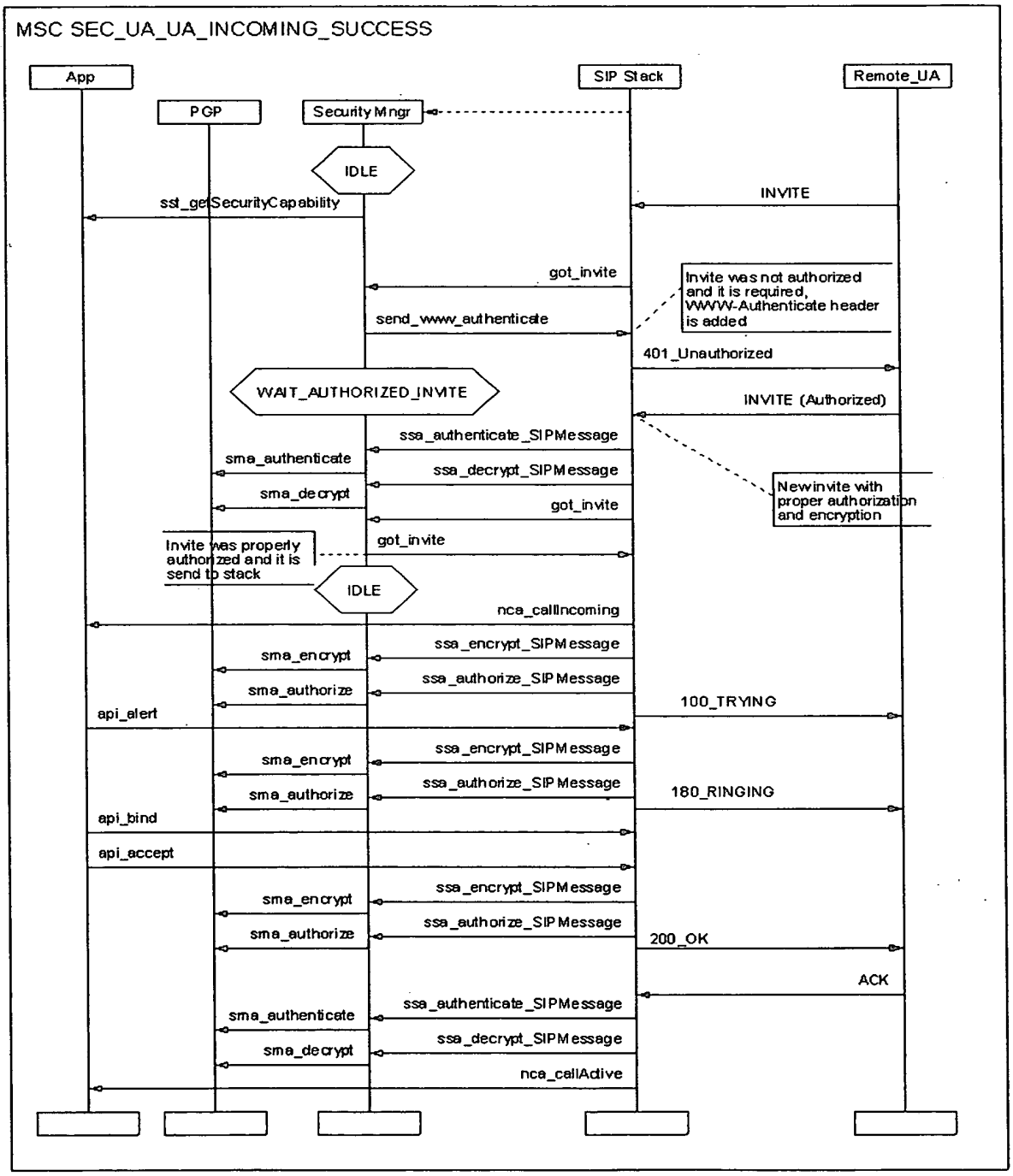

MSC SEC_UA_UA_INCOMING_SUCCESS
App
PGP
Security Mngr
SIP Stack
Remote_UA
IDLE
INVITE
ssl_getSecurityCapability
got_invite
Invite was not authorized and it is required, WWW-Authenticate header is added
send_www_authenticate
401_Unauthorized
WAIT_AUTHORIZED_INVITE
INVITE (Authorized)
ssa_authenticate_SIPMessage
sma_authenticate
ssa_decrypt_SIPMessage
sma_decrypt
got_invite
Newinvite with proper authorization and encryption
got_invite
Invite was properly authorized and it is send to stack
IDLE
nca_callIncoming
ssa_encrypt_SIPMessage
sma_encrypt
ssa_authorize_SIPMessage
sma_authorize
100_TRYING
api_alert
ssa_encrypt_SIPMessage
sma_encrypt
ssa_authorize_SIPMessage
sma_authorize
180_RINGING
api_bind
api_accept
ssa_encrypt_SIPMessage
sma_encrypt
ssa_authorize_SIPMessage
sma_authorize
200_OK
ACK
ssa_authenticate_SIPMessage
sma_authenticate
ssa_decrypt_SIPMessage
sma_decrypt
nca_callAdive

FIG. 21

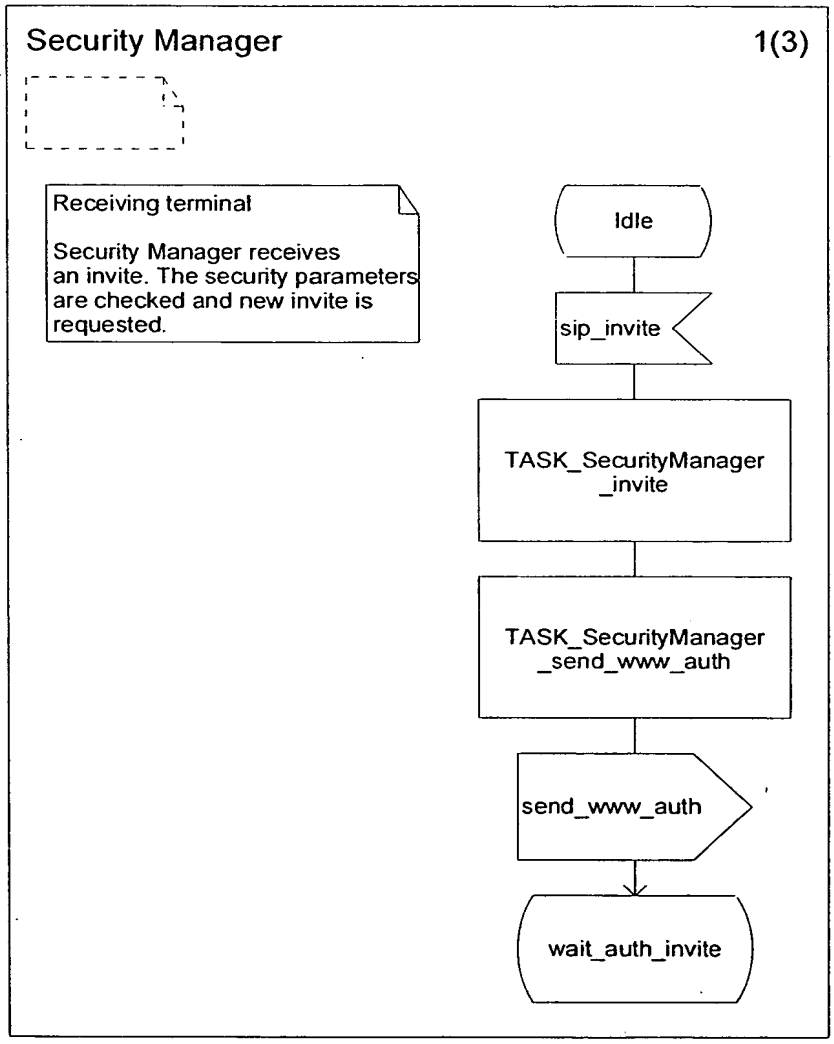
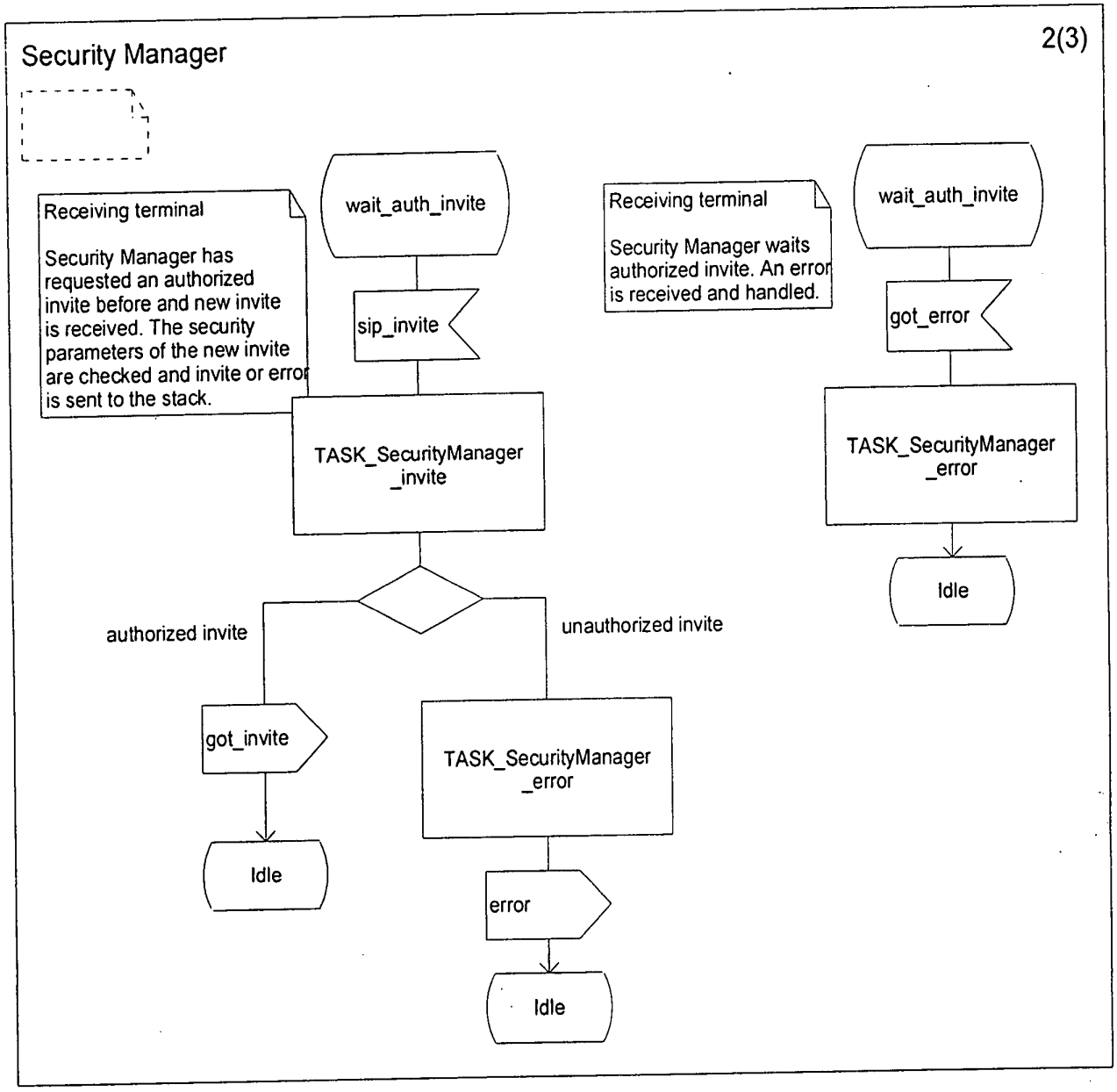

Security Manager
1(3)
Receiving terminal
Security Manager receives an invite. The security parameters are checked and new invite is requested.
Idle
sip_invite
TASK_SecurityManager _invite
TASK_SecurityManager _send_www_auth
send_www_auth
wait_auth_invite

FIG 22(a)

FIG 22(b)


Security Manager
2(3)
Receiving terminal
Security Manager has requested an authorized invite before and new invite is received. The security parameters of the new invite are checked and invite or error is sent to the stack.
wait_auth_invite
sip_invite
TASK_SecurityManager _invite
authorized invite
unauthorized invite
got_invite
Idle
TASK_SecurityManager _error
error
Idle
Receiving terminal
Security Manager waits authorized invite. An error is received and handled.
wait_auth_invite
got_error
TASK_SecurityManager _error
Idle

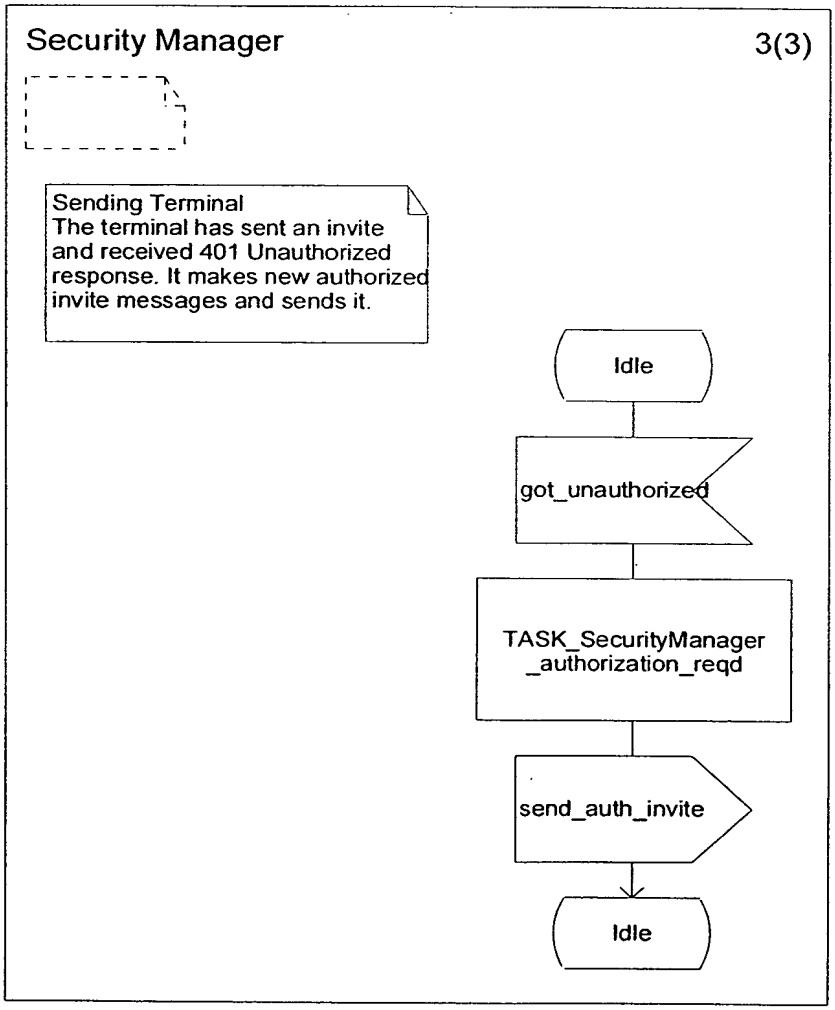

Security Manager
3(3)
Sending Terminal
The terminal has sent an invite and received 401 Unauthorized response. It makes new authorized invite messages and sends it.
Idle
got_unauthorized
TASK_SecurityManager _authorization_reqd
send_auth_invite
Idle

FIG 22(c)